Volume 111
Issue 3 *Dickinson Law Review - Volume 111, 2006-2007*

1-1-2007

Protecting the Most Valuable Corporate Asset: Electronic Data, Identity Theft, Personal Information, and the Role of Data Security in the Information Age

Kenneth M. Siegel

Protecting the Most Valuable Corporate Asset: Electronic Data, Identity Theft, Personal Information, and the Role of Data Security in the Information Age

Kenneth M. Siegel*

I. Introduction

A. Today's Business Environment: No Longer Defined by Bricks and Mortar

As new technologies have developed, business processes have changed dramatically. Changes in technology continue to allow businesses to increase efficiency, increase productivity, manage supply and distribution chains, interact with customers, and increase profitability. Today, a consumer might purchase an item from a company using the company's e-commerce website. The consumer pays with a credit card and can track the order until it reaches his or her door. The seller uses sophisticated software management programs that simultaneously update inventory when the order is shipped and reorder from suppliers if inventory levels are too low. In some cases, the seller's software programs communicate with its business partners and items the seller does not yet have in inventory are shipped directly to the consumer. At the same time, the company's financial records are updated with sales and any purchases of raw goods. In many cases, funds are transferred electronically.

Technology has not only created an online marketplace; it has also redefined the process by which traditional "brick and mortar" companies, and even service businesses, operate. Customers can swipe a debit card

* J.D. Candidate, The Dickinson School of Law of the Pennsylvania State University, (2007); M.S.I.S. Candidate, Pennsylvania State University, The Capital College, (2007); B.S., Management Information Systems, Gannon University *summa cum laude* (2004).

and automatically pay for a purchase. They can check their bank accounts online. Consumers can use their cellular phones to place orders and their laptop computers to conduct business during their lunch break at the park.

As technology has changed the business landscape, the risk management concerns of companies utilizing technology have changed as well. Protecting consumer data is no longer a matter of locking the file cabinet. At one time technology was used to keep and manage only internal company records, so securing internal databases might have been the chief method by which companies protected consumer information. This is no longer the case, as companies make customer information available to business partners using the Internet. Data is also exchanged through wireless connections and shared between companies or divisions located in different countries.

What must a company do to protect its customers' personal data? What does the law require? Is it feasible for the law to make technology-specific requirements when technology is often replaced by new technology every few years or even months?

B. Information: The Catalyst of Today's Business Environment

Identity theft is a serious problem, which can affect even the most sophisticated consumers.[1] Over nine million Americans were victims of identity theft in 2004.[2] Identity theft, in the United States, has cost nearly $53 billion each year over the last three years.[3] Consumers pay $5 billion of that cost directly.[4] The rest is paid by businesses and is absorbed indirectly by consumers in the form of higher prices.[5] Despite the fact that criminals have a thorough understanding of the value of personal information, law enforcement is not very successful at catching criminals who commit identity theft.[6] Less than 1 in 700 identity crimes ends with a conviction.[7] In addition to suffering monetary loss, the

1. Steven Levy & Brad Stone, *Grand Theft Identity*, NEWSWEEK, Sept. 5, 2005, at 38. This article discusses the story of Deborah Platt Majoras, a recent victim of identity theft. Majoras, coincidentally, is the chairperson of the federal agency most concerned with identity theft, the Federal Trade Commission. *Id.*

2. JAVELIN STRATEGY & RESEARCH, 2005 IDENTITY FRAUD SURVEY REPORT 11 (2005), http://www.javelinstrategy.com/reports/2005IdentityFraudSurveyReport.html (last visited Nov. 1, 2006) [hereinafter 2005 IDENTITY FRAUD SURVEY].

3. *Id.* at 3.

4. Levy & Stone, *supra* note 1.

5. *Id.*

6. *See, e.g.*, Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1074-75 (2001) (discussing impediments to the successful enforcement of cybercrime).

7. *Id.*

typical victim of identity theft can expect to devote about 175 hours investigating and filling out paperwork to recover from identity theft, sometimes dealing with the repercussions for several months or even years.[8]

The good news, at least from the perspective of an information technology ("IT") manager, is most thieves still steal personal information through off-line rather than online methods.[9] The likelihood of large losses is still greater from off-line theft than online theft.[10] However, recent breaches in data security suggest this is about to change. In August 2005, Sunbelt Software, a security firm, discovered passwords for online accounts and credit card numbers stolen by a Trojan virus[11] stored on a server in the United States.[12] In June 2005, forty million Discover, Visa, MasterCard, and American Express numbers were potentially exposed to hackers[13] because of insufficient security by a company called CardSystems.[14] The large number of individuals potentially affected by recent data breaches and the realization that theft from large data warehouses could drastically increase the amount of data stolen during a single security breach have created a need to make electronically collected and stored personal information more secure.[15] Additionally, these events have led some to question what corporations

8. *Id.*

9. *See* 2005 IDENTITY FRAUD SURVEY, *supra* note 2, at 3-4.

10. *Id.* In cases where the method of theft was known, 68.2% of stolen information was obtained off-line, compared to 11.6% obtained online. *Id.* Mean loss from information stolen by fraudulent email solicitations was $2,320, while information taken from the theft of paper mail was $9,243, and information stolen from family and friends was $15,607. *Id.* This discrepancy makes sense when one considers that the detection time for online transactions is much less than paper transactions. For example, the mean fraud detection time in cases involving paper statements mailed on a thirty-day cycle was 114 days compared to 18 days for detection in cases where consumers monitored their accounts through the Internet or using an ATM. *Id.* Sadly, family and friends account for over half of all identity theft. *Id.*

11. A Trojan virus is named after the Greek war story, in which soldiers hid inside a wooden horse to enter the enemy city. GERALD V. POST & DAVID L. ANDERSON, MANAGEMENT INFORMATION SYSTEMS: SOLVING BUSINESS PROBLEMS WITH INFORMATION TECHNOLOGY 173, 588 (4th ed. 2006). Similarly, a Trojan virus is malicious code that is hidden inside another program. *Id.* When the main program is run, the malicious code is also run, usually without the user's knowledge. *Id.* The malicious code then might delete files, display messages, or capture data and transmit it to an external source. *Id.*

12. Levy & Stone, *supra* note 1.

13. In addition to the common understanding that a "hacker" is someone who breaks into computer systems, the term "hacker" can also refer to "someone who learns about computer code, networks, and systems in an effort to understand them and correct errors." TAMARA DEAN, ENHANCED NETWORK+ GUIDE TO NETWORKS 758 (2003). In this comment, "hacker" will be used, in the way it is commonly understood by the public, to mean someone who attempts to exploit code or a network for malicious purposes.

14. Levy & Stone, *supra* note 1.

15. *Id.*

are doing to secure personal data.[16]

The Federal Trade Commission ("FTC"), under its authority of Section 5 of the FTC Act,[17] which prohibits unfair or deceptive practices, has brought cases against corporations failing to live up to their promises about the security they provide for consumer information.[18] While companies that maintain financial[19] and health information[20] must comply with specific security requirements, companies collecting and maintaining other types of information must comply only with the promises they make to their customers.[21] This Comment will evaluate the need for corporations to develop and implement security programs that protect consumer data and the need for uniform legislation that provides minimum requirements for all entities that collect personal information from consumers. Part II will examine the importance of electronic data in today's corporate environment and outline the potential risks associated with using electronic data. Part III will explore the data security requirements that exist under current law. Part IV will look at recent actions taken by the FTC to protect consumer data in situations where the law does not currently require specific security measures. An analysis of the action taken by the FTC will help determine what a corporation should consider when developing a data security program. Part V will recommend considerations that legislation directed at electronic data security should address. From these considerations, companies that are interested in developing data security systems and consumers who are concerned about losing their personal data should be able to formulate effective plans of action for future transactions involving electronic data. Part VI concludes.

II. Background

> The flow of information on the characteristics of customers, both businesses and individuals, and changes in information technology in recent years, have improved the efficiency, innovativeness and competitiveness of our markets. This information has enabled producers and marketers to fine-tune production schedules to the ever

16. *Id.*

17. 15 U.S.C. § 45(a)(1) (2006).

18. Federal Trade Commission, Privacy Initiatives, http://www.ftc.gov/privacy/privacyinitiatives/promises.htm (last visited Oct. 29, 2005) [hereinafter FTC Privacy Initiatives].

19. Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809 (2006).

20. Health Insurance Portability and Accountability Act of 1996, Pub. Law 104-191, 110 Stat. 1936 (codified in scattered sections of 42 U.S.C.).

21. FTC Privacy Initiatives, *supra* note 18.

> greater demands of our consuming public for diversity and individuality of products and services.[22]

Today it is estimated that eighty percent of corporate assets are digital.[23] As a result of the prevalence of electronic assets, security of data, networks, and software applications has become an issue that must be addressed from an organizational risk management level.[24] Over sixty data breaches occurred in the first half of 2005 alone.[25] Consequently, over fifty million personal records have been exposed to possible criminal misuse.[26] As former Chairman Greenspan suggests, information drives today's markets.[27] E-business has increased efficiency and profitability and created better customer service.[28] However, e-business has also brought sensitive consumer data online, where it might be exposed to theft or manipulation.[29]

Reports of identity theft have inundated the media in the last year.[30] However, identity theft was prevalent even before the recent media attention.[31] In 2002, for example, there were twice as many reported

---

22. Alan Greenspan, Fair Credit Reporting Act question submitted to Chairman Greenspan in writing following February 12, 2003 hearing, House Financial Service Committee response received Feb. 28, 2003, *available at* http://www.protectconsumercredit.org/what others/Greenspan.asp.

23. JODY R. WESTBY, ROADMAP TO AN ENTERPRISE SECURITY PROGRAM 12 (2005) [hereinafter WESTBY].

24. *Id.*

25. Press Release, Vontu, Vontu Introduces the Industry's Only Solution to Discover, Monitor, and Prevent Loss of Consumer Data and Intellectual Property (July 25, 2005), *available at* http://www.vontu.com/news/release_ detail.asp?id=314.

26. *Id.*

27. *See* Greenspan, *supra* note 22.

28. John R. Vacca, *Securing "Open" Corporate Networks*, E-BUSINESS ADVISOR, Aug. 2002, at 33.

29. *See* Press Release, Kavado, Why Network Security is not Enough: Kavado and Security Innovation to Co-Host Free Webcast (March 1, 2005), *available at* http://www.kavado.com/news/press-release-detail.asp?id=66.

30. On February 15, 2005, ChoicePoint announced that it had suffered a data breach that could affect nearly 150,000 individuals. A Chronology of Data Breaches Reported Since the ChoicePoint Incident (2005), http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Nov. 1, 2006). Since ChoicePoint's announcement many other companies have followed ChoicePoint's lead, establishing disclosure as the "best-practice" of the industry. *Id.* Corporate, educational, and government organizations have announced breaches that exposed over fifty-two million accounts to fraud between February of 2005 and the end of that year. *Id.*

Some of the more notable data breaches were announced by Bank of America, MCI, and LexisNexis. *Id.* MasterCard International announced the largest exposure of the year in June of 2005. Robert Berner & Adrienne Carter, *Swiping Back at Credit-Card Fraud; Bogus transactions are falling overall, but e-tailers are still feeling the pain*, BUSINESS WEEK, July 11, 2005, at 72. One of the companies that processed transactions for MasterCard suffered a security breach that exposed more than forty million accounts to fraud. *Id.*

31. *See Identity Theft Surveys and Studies: How Many Identity Theft Victims Are*

cases of identity theft than traditional robberies.[32] While the low conviction rate of identity theft can be blamed on the technology that is being used to track and trace security breaches and cyber attacks, the high occurrence rate cannot.[33] Identity theft can be partially blamed on corporations engaging in data sensitive transactions without maintaining adequate security programs.[34]

A. How Theft of Personal Data Occurs

There are two main types of identity theft: "account takeover" and "application fraud."[35] "Account takeover" occurs when existing account information is stolen.[36] All that is needed to make a fraudulent purchase is a credit card, or a credit card number and an expiration date.[37] Application fraud is even easier to commit and more difficult to discover.[38] A thief can commit application fraud with as little information as a social security number and name.[39] There are several methods used by thieves to obtain personal information.[40] Thieves have bought information from employees, stolen it from trucks, stolen hardware containing information, and taken advantage of corporations' failures to adequately secure data.[41]

1. "Low-tech" Identity Theft: Old Fashioned Theft

While "high-tech" or electronic methods of identity theft have recently dominated the news and pose a serious future threat, the majority of identity theft in the United States still occurs through "low-

---

There? (2005), http:www.privacyrights.org/ar/idtheftsurveys.htm [hereinafter Identity Theft Surveys and Studies] (last visited Jan. 4, 2006) (noting that 27.3 million Americans have been victims of identity theft over the last five years).

32. *See* WESTBY, *supra* note 23, at vii.

33. *See id.*

34. *See id.*

35. Privacy Rights Clearinghouse, *Reducing the Risk of Identity Theft* (2005), http://www.privacyrights.org/fs/fs17-it.htm. (last visited November 21, 2006) [hereinafter Reducing the Risk].

36. *Id.*

37. *Id.*

38. *See id.* Account takeover is easier to discover, because false charges show up on a monthly account statement. *Id.* On the other hand, when application fraud occurs, the monthly statements are sent to the impostor who assumed the victim's identity when he or she created the account. Therefore, victims might not learn of application fraud for some time. *Id.*

39. *See* Kurt M. Saunders & Bruce Zucker, *Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act*, 8 CORNELL J.L. & PUB. POL'Y 661, 668 (1999) (discussing a simple method by which a thief could obtain a new account).

40. *See generally* Levy & Stone, *supra* note 1.

41. *Id.*

tech" methods.[42] Lost or stolen wallets account for over one-fourth of lost identity cases.[43] Thieves commonly obtain personal information through "dumpster-diving;" less artfully known as rooting through trash bins to find documents containing personal information.[44] Friends and relatives who have access to personal information often take advantage of the trust bestowed upon them.[45] Thieves find information through public records, or might pose as an employer or landlord to obtain information that cannot be found in public records.[46] Thieves use these and other methods[47] to obtain personal information; in many situations, however, technology now provides the ability to obtain similar results faster and in larger volumes.[48]

2. "High-tech" Identity Theft: Electronic Dumpster Diving

Thieves use technology to directly steal personal information through keylogging,[49] spyware,[50] and phishing.[51] Among these methods, phishing has recently become the most common.[52] Phishing involves sending consumers email that is designed to look like it is from a legitimate company.[53] Thieves simply ask the consumer to update or verify their information and up to five percent of the recipients comply.[54] When the fraudulent email is sent to a consumer who is concerned about identity theft, but perhaps not educated about how it occurs, the suggestion that a company they trust needs to verify personal information seems reasonable.[55] The consumer responds under the belief that they

42. *See* 2005 IDENTITY FRAUD SURVEY, *supra* note 2, at 3-4.
43. *Id.* at 6.
44. Reducing the Risk, *supra* note 35.
45. 2005 IDENTITY FRAUD SURVEY, *supra* note 2, at 7.
46. Reducing the Risk, *supra* note 35.
47. Other common methods employed by thieves to steal people's identity include stealing mail, accessing the information as part of a legitimate transaction, obtaining personal identification numbers by "shoulder surfing" at ATMs, and stealing files from the workplace. *See generally* 2005 IDENTITY FRAUD SURVEY, *supra* note 2, at 7; Reducing the Risk, *supra* note 35.
48. See Levy & Stone, *supra* note 1 (stating that criminals are now able to grab information in large quantities instead of obtaining it victim-by-victim).
49. Keylogging involves a computer program, installed without the user's knowledge, that records all the keystrokes made by the user. 2005 IDENTITY FRAUD SURVEY, *supra* note 2, at 6.
50. Spyware is often installed without the user's knowledge. Once installed, it captures the activities of the user, such as the websites visited, passwords entered, and other personal information. The spyware then sends this information to a website where it is collected by a third party. POST & ANDERSON, *supra* note 11, at 173.
51. 2005 IDENTITY FRAUD SURVEY, *supra* note 2, at 6.
52. Levy & Stone, *supra* note 1.
53. *Id.*
54. Identity Theft Surveys and Studies, *supra* note 31.
55. Levy & Stone, *supra* note 1.

are helping to protect themselves from becoming a victim of fraud.[56] Unfortunately phishing websites are hard to shut down because they usually are hosted overseas and the thieves that run them keep them online for an average of only 2.25 days.[57]

Thieves also use technology to sell stolen information and to use stolen credit card numbers to make fraudulent purchases.[58] Thieves sell stolen records using chat rooms and, in some cases, advertise the stolen information on websites.[59] Since Internet purchases are Cardholder-Not-Present ("CNP") transactions,[60] it is easy for a thief to use stolen credit card numbers along with personal information to make fraudulent Internet purchases.[61] Technology helps crooks avoid detection as well. Thieves sell items that they do not own in online auctions, then they use stolen credit card information to purchase the items from a legitimate retailer when the auction closes.[62] The legitimate retailer then ships the items to the auction winner, allowing the thieves to collect the auction price without exposing themselves to detection.[63]

The method of electronic theft most dangerous to consumers is a direct attack on corporate databases.[64] Unlike phishing, keylogging, and the "low-tech" methods of obtaining information discussed above, a single direct database attack can affect millions of consumers.[65] Consumers who take measures to protect their data or who do not use online transactions may not need to be as concerned about other methods of fraud as consumers who are careless or uneducated about identity theft. However, a direct database attack affects all consumers equally since most organizations consolidate all of their data regardless of how the information was collected.[66]

---

56. *Id.*

57. Identity Theft Surveys and Studies, *supra* note 31.

58. Levy & Stone, *supra* note 1.

59. *Id.*

60. CNP transactions, as opposed to cardholder-present transactions, take place remotely and neither the cardholder nor the card is present at the point-of-sale. The seller is unable to check the card and the identity of the cardholder because these transactions occur remotely. The relative ease of CNP fraud compared to cardholder-present fraud, combined with the reality that more transactions are being performed as CNP transactions has led to a rise in CNP fraud. Paul Meadowcroft, *Combating Cardholder not Present Fraud*, IT OBSERVER, October 17, 2005, http://www.ebcbg.com/articles.php?id=940.

61. *Id.*

62. Berner & Carter, *supra* note 30, at 72.

63. *Id.*

64. Criminals use automated software called "bots" to probe the Internet for vulnerable databases. Most often, criminals are able to enter a database through a security flaw that could have been prevented. Levy & Stone, *supra* note 1.

65. *Id.*

66. *See* 2005 IDENTITY FRAUD SURVEY, *supra* note 2, at 6.

B. Protecting Electronic Data

To effectively protect electronic data, both privacy and security issues must be considered.[67] Security is the foundation of privacy and prevention of electronic crime.[68] Privacy of electronic information has been a concern since information management systems took a prominent role in business processes.[69] Without fully exploring the entire realm of either issue, a brief look at the privacy and security concerns facing organizations helps one understand the complexity of developing an effective data security system. The issues privacy and security present to an organization also foster an understanding that the protection of electronic data is more than an "IT issue" and instead must be approached from an "organization-wide" standpoint.

1. Privacy

Personal privacy concerns existed well before the birth of the Internet. However, the speed at which data can be transmitted using modern technology[70] and the amount of personal information that can be stored in electronic databases[71] has magnified these concerns.[72] Corporations not only have to be aware of customers' personal privacy concerns, they also must consider contractual obligations, legal requirements, and information unique to their business objectives.[73] From a corporate perspective, privacy is a strategic business issue because information is an important asset. Privacy considerations determine, in part, what a corporation can do with information assets without incurring legal liability or harming its image.

Several solutions have been proposed to confront privacy concerns, including stricter laws, a greater call for self-regulation from the private sector, and technology-driven solutions.[74] Regardless of future attempts

---

67. *See generally* JODY R. WESTBY, INTERNATIONAL GUIDE TO CYBER SECURITY (2004) [hereinafter WESTBY, SECURITY] (in order for the Internet to prosper individual users, governments, and businesses must work together to create effective security programs); JODY R. WESTBY, INTERNATIONAL GUIDE TO PRIVACY (2004) [hereinafter WESTBY, PRIVACY] (businesses must consider privacy issues when developing security programs).

68. WESTBY, SECURITY, *supra* note 67, at xxxi.

69. WESTBY, PRIVACY, *supra* note 67.

70. "Communications privacy" is a classification that includes electronic surveillance, encryption, email, and digital telephony. DUNCAN LANGFORD, INTERNET ETHICS 71 (2000) [hereinafter LANGFORD].

71. "Information privacy" includes issues associated with personal information stored in electronic medium. *Id.*

72. *See id.* at 72.

73. WESTBY, PRIVACY, *supra* note 67, at 135.

74. LANGFORD, *supra* note 70, at 83.

to preserve privacy, companies interested in implementing effective data security programs should conduct a privacy risk assessment.[75] Certainly industry best practices provide a starting point for a company when developing a privacy policy, but privacy laws, regulations, and strategic decisions dependent on factors unique to individual businesses also must be considered.[76] Some of these factors include the method of information collection, the physical location of the business and its customers, the type of information collected, and the industry to which the company belongs.[77] Only after determining its privacy goals and requirements can a company determine how to effectively protect its information.[78]

2. Security

E-business cannot be successful if the public cannot trust a company's information systems to protect their personal information.[79] While privacy might be seen as a more personal or organization-specific issue, the interconnectivity of the Internet has made security a global issue.[80] The security of cyberspace extends far beyond issues of individual privacy and the protection of corporate secrets and encompasses national defense, terrorism, and the national and global economies.[81] In order to continue to promote trust in information systems, these broader issues should be considered as companies approach their individual data security concerns.[82]

A lack of coordination between privacy goals and information security systems can be problematic; unfortunately it is common because many organizations tend to approach privacy and security issues independently.[83] An effective security program should include policies and procedures designed to serve the unique needs of the particular organization in tandem with the organization's privacy concerns.[84]

---

75. WESTBY, PRIVACY, *supra* note 67, at 135.
76. *Id.* at 138.
77. *Id.* at 139.
78. *Id.* at 136.
79. WESTBY, SECURITY, *supra* note 67, at 154.
80. *Id. See also The National Strategy to Secure Cyberspace* at 1073, 1077 (PLI Patents, Trademarks, and Literary Property Course Handbook Series Order No. G0-018F, 2003) [hereinafter *The National Strategy to Secure Cyberspace*] (threats to cyberspace have risen in recent years and vulnerabilities must be reduced to protect the United States since the operations of information systems drives much of the country's critical infrastructure).
81. *See The National Strategy to Secure Cyberspace, supra* note 80, at 1077.
82. WESTBY, SECURITY, *supra* note 67, at 154.
83. WESTBY, PRIVACY, *supra* note 67, at 137.
84. WESTBY, SECURITY, *supra* note 67, at 188.

While impressive technology solutions[85] are available to secure data, software, and networks, the needs of the organization have to drive the implementation of security mechanisms in order for a security program to be successful and cost effective.[86] Rapid changes in technology and business requirements call for organizations to make security an integral part of their planning and operations.[87]

Although security of information systems and electronic data is accomplished by the implementation of technology solutions, security should be viewed as an enterprise-wide issue.[88] Many security programs are managed from an IT perspective; this approach can ignore the managerial, operational, and legal issues that should be considered in order to provide effective security.[89] An enterprise-wide approach to security effectively accounts for legal, regulatory, and contractual obligations, as well as best practices, in a way that an IT-only approach cannot.[90] The need for effective privacy planning and security policies is more important to private organizations today than ever before.[91] The importance of electronic data and the ability to transfer data using computer systems has become essential to our economy.[92] Concern about the protection of electronic resources will only continue to grow as both the public[93] and private sectors work together to protect electronic

85. Secure technology used for authorization includes password protection, biometric identifiers, and smartcards. *Id.* Other methods used to secure data and networks include firewalls, antivirus software, backup systems and procedures, intrusion detection systems, filtering systems to keep employees from exporting sensitive data, several methods of encryption technology, unique authentication requirements, and digital signatures. LANGFORD, *supra* note 70, at 166-73.

86. WESTBY, SECURITY, *supra* note 67, at 188.

87. *See* Wendy Tanaka, *Blue Bell, Pa.-Based Unisys Will Offer Package of Internet-Security Services*, PHILADELPHIA INQUIRER, Apr. 2, 2001, at D03.

88. WESTBY, SECURITY, *supra* note 67, at 188.

89. WESTBY, *supra* note 23, at 4.

90. WESTBY, SECURITY, *supra* note 67, at 188.

91. *See The National Strategy to Secure Cyberspace*, *supra* note 80, at 1081.

92. *See id.*

93. The Internet has been described as a "critical infrastructure" that is as important to national defense and the economy as roads, bridges, and other components of the nation's physical infrastructure. *See* Emily Frye, *The Tragedy of the Cybercommons: Overcoming Fundamental Vulnerabilities to Critical Infrastructures in a Networked World*, BUSINESS LAWYER, November 2002, at 349. However, the Internet was not created with security in mind. *Id.* at 351. Transmission Control Protocol / Internet Protocol (TCP/IP), the communication mechanism upon which the Internet operates, was designed for usability and availability, not security. *Id.* at 353. The national economy has been changed by the use of networked computer systems and the ability to transfer data using them; however, security was not a concern during the early days of computer use, leaving many security issues unanswered. *See* id. at 351. Computer systems open and close pipelines, control manufacturing processes, operate utility grids, and are vital to air traffic control. The U.S. banking system electronically moves approximately $3 trillion every day. WESTBY, SECURITY, *supra* note 67, at 11.

data and computer networks.[94]

III. Current Data Security Requirements: Data Protected By Legislation

A. The Gramm-Leach-Bliley Act[95]

The Financial Modernization Act of 1999, better known as the "Gramm-Leach-Bliley Act" ("GLB Act"), includes provisions to protect consumer information held by financial institutions.[96] Under the GLB Act, companies that are "significantly engaged"[97] in "financial activities"[98] are required to give consumers privacy notices which explain the information sharing practices of the company.[99] Customers also have the right to limit some information sharing by the company.[100] Further, any entity that a financial institution shares consumer information with may be restricted in its use and disclosure of that information.[101]

The GLB Act's Privacy Rule applies to financial institutions that collect "nonpublic personal information"[102] from its "customers" or

94. WESTBY, SECURITY, *supra* note 67, at 19.

95. Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809 (2006).

96. FTC Privacy Initiatives, *supra* note 18.

97. The FTC's "significantly engaged" standard accounts for all of an organization's financial activities to determine whether the organization is "significantly engaged" in financial activities; however, two factors carry particular importance in determining whether the "significantly engaged" standard is met. *How to Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act* (2002), http://www.ftc.gov/bcp/conline/pubs/buspubs/glblong.pdf at 6 [hereinafter *How to Comply*]. The first factor is the existence of a formal agreement. *Id.* If the organization has a formal agreement with customers it is more likely to meet the "significantly engaged" standard. *Id.* The second factor is the frequency that the organization engages in the financial activity. *Id.* If the organization regularly engages in the financial activity in question, it is likely that the "significantly engaged" standard is met. *Id.*

98. The activities that an organization engages in determine whether it is a financial institution. Financial activities include: lending, exchanging, transferring or investing for others; safeguarding money or securities; providing financial, investment, or economic advisory services; brokering loans; servicing loans; collecting debts; providing real estate settlement services; and even providing career counseling for individuals seeking employment in the financial services industry. *Id.* The FTC has also interpreted the term "financial institution" to include law firms. WESTBY, PRIVACY, *supra* note 67, at 19- 20.

99. *How to Comply*, *supra* note 97, at 5.

100. *In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act*, http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.pdf (last visited Nov. 20, 2006).

101. *How to Comply*, *supra* note 97, at 5.

102. "Nonpublic personal information" is financial information

(i) provided by a consumer to a financial institution;

(ii) resulting from any transaction with the consumer or any service performed

"consumers" and companies that receive "nonpublic personal information" from financial institutions.[103] The frequency and type of notification requirements that an organization must send depend upon whether the "nonpublic personal information" in question belongs to a "customer" or a "consumer."[104] The GLB Act defines a "consumer" as "an individual[105] who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes. . . ."[106] "Customers" are "consumers" who have a continuing relationship with the financial institution.[107] Regardless of whether a financial institution plans to disclose "nonpublic personal information" it must "[a]t the time of establishing a customer relationship with a consumer and not less than annually during the continuation of such relationship . . . provide a clear and conspicuous disclosure to [the] customer."[108] This privacy notice must include the organization's policies and practices regarding disclosing nonpublic personal information to affiliates and third parties, disclosing nonpublic personal information of past customers, and the measures the organization takes to protect consumers' nonpublic personal information.[109] The GLB Act requires an organization to provide "consumers" with privacy notices only if they intend to share nonpublic personal information with third parties.[110]

A financial institution wishing to disclose nonpublic personal information must provide its "consumers"[111] with an opt-out notice.[112] The opt-out notice must "clearly and conspicuously disclose to the consumer . . . that . . . information may be disclosed to a third party"[113]

---

for the consumer; or

(iii) otherwise obtained by the financial institution

15 U.S.C. § 6809(4)(A) (2006). Any information that is publicly available is not "nonpublic personal information." *Id.* § 6809(4)(B). All information included in a list that contains or is derived from "nonpublic personal information" is considered to be "nonpublic personal information." *Id.* § 6809(4)(C).

103. *How to Comply*, *supra* note 97, at 2.

104. *Id.* at 3.

105. The Privacy Rule only applies to individuals; therefore, it does not protect information belonging to commercial consumers. *Id.*

106. 15 U.S.C. § 6809(9).

107. *How to Comply*, *supra* note 97, at 3.

108. 15 U.S.C. § 6803(a) (2006).

109. *Id.*

110. *How to Comply*, *supra* note 97, at 7.

111. 15 U.S.C. § 6809. The opt-out requirement applies equally to "customers" and "consumers." By definition, "customers" are a subclass of "consumers" and therefore any requirement applicable to "consumers" also includes "customers". *How to Comply*, *supra* note 97, at 3.

112. 15 U.S.C. § 6802(b)(1) (2006).

113. *Id.* § 6802(b)(1)(A).

and give the consumer an explanation of how he or she can exercise the opt-out choice.[114] The organization must give the consumer a reasonable opportunity to exercise the opt-out option before it can disclose any information.[115] The GLB Act does not require that an organization provide its consumers with an opt-out choice if it is providing nonpublic personal information to a third party in order for the third party to perform services on behalf of the organization.[116] However, the organization must fully disclose that it is providing the information, and enter into a contractual agreement with the third party requiring the third party to maintain the confidentiality of the information.[117]

After an organization discloses information to a third party, that third party can again disclose the information, but only in accordance with the privacy policy of the original organization.[118] The third party can still disclose information to its affiliates and to the affiliates of the original institution if the disclosure could be made by the original institution.[119] Additionally, the third party can disclose information if it provides the consumer with an opportunity to opt out and the consumer does not do so.[120]

In addition to the notice requirements of the Privacy Rule, the GLB Act also includes the Safeguards Rule.[121] The Safeguards Rule requires financial institutions to design, implement, and maintain safeguards to secure customer records and information.[122] The Safeguards Rule applies to an organization's "customer" information and to any "customer" information provided to the organization by another company.[123] The Safeguards Rule requires an organization to maintain a written "information security program . . . [that] contains administrative, technical, and physical safeguards. . . ."[124] The objectives of the Safeguards Rule are to provide for the security of customer information, protect against security and integrity hazards, and protect against

114. *Id.* § 6802(b)(1)(C).
115. *Id.* § 6802(b)(1)(B).
116. *Id.* § 6802(b)(2).
117. 15 U.S.C. § 6802(b)(2).
118. *Id.* § 6802(c).
119. *How to Comply*, *supra* note 97, at 13.
120. 15 U.S.C. § 6802 (2006).
121. 15 U.S.C. § 6801(b).
122. FTC Standards for Safeguarding Customer Information, 16 C.F.R. § 314.1(a) (2006).
123. *Id.* § 314.1(b).
124. *Id.* § 314.3(a). These safeguards include designating an employee or employees to coordinate the information security program and conducting a risk assessment of, at least, the following: employee training, information systems, and detection and prevention of attacks and system failures. *Id.* §§ 314.3(a)-(b).

unauthorized access to customer data.[125] The Safeguards Rule is designed to be flexible so as to be equally applicable to organizations of different sizes.[126] The information security program "shall . . . [be] appropriate to [the organization's] size and complexity, the nature and scope of [the organization's] activities, and the sensitivity of any customer information at issue."[127]

While the GLB Act does provide some protection for consumers, it still allows for companies to disclose or even sell information.[128] First, the GLB Act is limited in scope. It only applies to organizations "significantly engaged" in "financial activities."[129] It only applies to "nonpublic personal information."[130] Annual notice must be given only to "customers," potentially leaving "consumers" unaware of the privacy policies of an organization that possess the consumer's information.[131] An organization is free to disclose information to third parties as long as it contracts with the third party to maintain the confidentiality of the information.[132] This means that a consumer who conscientiously discloses information to his or her financial organization cannot control the further dissemination of his or her personal information. As it stands, a consumer's information might be sitting in several databases belonging to any number of organizations possessing information security policies unknown to the consumer.[133]

Secondly, the GLB Act's opt-out requirement allows an organization to disclose almost any information[134] if the consumer fails to exercise his or her opt-out rights. Often consumers do not exercise these rights.[135] Privacy notices are written at a graduate reading level,[136] are long,[137] and often are used as a marketing ploy by the companies

125. *Id.* § 314.3(b).
126. *Id.* § 314.3(a).
127. *Id.*
128. Eric Poggemiller, *The Consumer Response to Privacy Provisions in Gramm-Leach-Bliley: Much Ado About Nothing?*, 6 N.C. BANKING INST. 617, 633 (2002).
129. 15 U.S.C. § 6809(3) (2006).
130. *Id.* at § 6801(a).
131. *Id.* at § 6802(b)(1).
132. *Id.* at § 6802(b)(2).
133. 16 C.F.R. § 314.3(a) (2006). The Safeguards Rule provides some comfort in the area of information security; however, it only requires an organization to develop a security program that is appropriate to its size and structure. *Id.*
134. 15 U.S.C. § 6802(d) (2006). Account numbers or similar access numbers or codes cannot be disclosed for marketing purposes regardless of whether the consumer has exercised his or her opt-out rights. *Id.*
135. *See* Poggemiller, *supra* note 128, at 628.
136. *Id.* at 629.
137. *See id.* at 631 (suggesting that some companies deliberately create long and confusing notices).

issuing them.[138] While it is possible that some consumers are indifferent to information sharing or feel that information sharing is beneficial, it is clear that many consumers are unaware of their opt-out rights under the GLB Act.[139]

The Safeguards Rule forces an organization to focus on important objectives when creating and implementing an information security plan.[140] The Safeguards Rule does not provide specific technical standards that an organization must meet in order to comply, instead it requires an information security program that is appropriate for the particular organization.[141] While this flexibility does not leave a company with an item-by-time checklist of what it must do to comply, the Safeguards Rule does provide minimum considerations for a company's risk assessment.[142] Most companies also realize that providing adequate security for customer information makes good business sense.[143] This realization, combined with the requirements of the Safeguards Rule, provides companies with an incentive to actively pursue an effective data security program.

B. HIPAA

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[144] authorized the Department of Health and Human Services ("HHS") to issue privacy protections for patients' health care information.[145] The goal of HIPAA is to improve "the efficiency and effectiveness of the health care system by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information."[146] In order to further this goal and protect "individually

138. *Id.* at 632.

139. *See* R. Bradley McMahon, *Note: After Billions Spent to Comply with HIPAA and GLBA Privacy Provisions, Why is Identity Theft the Most Prevalent Crime in America?* 49 VILL. L. REV. 625, 641-42 (2004) (suggesting that many consumers do not exercise their opt-out rights because the process is difficult and cumbersome.)

140. *See* FTC Standards for Safeguarding Customer Information, 16 C.F.R. § 314.3(a).

141. *Id.*

142. WESTBY, PRIVACY, *supra* note 67, at 30-31.

143. Financial Institutions and Customer Data: Complying with the Safeguards Rule (2002), http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.pdf 1 [hereinafter Financial Institutions].

144. Health Insurance Portability and Accountability Act of 1996, Pub. Law 104-191, 110 Stat. 1936 [hereinafter HIPAA] (codified in scattered sections of 42 U.S.C.).

145. Press Release, U.S. Dep't of Health and Human Services, *Fact Sheet: Protecting the Privacy of Patients' Health Information* (Apr. 14, 2003) *available at* http://www.hhs.gov/news/facts/privacy.html.

146. Pub. L. No. 104-191 § 261, 110 Stat. 2021 (1996).

identifiable health information,"[147] HHS issued the Standards for Electronic Transactions ("Transactions Rule"),[148] the Standards for Privacy of Individually Identifiable Health Information ("HIPAA Privacy Rule"),[149] and the Security Standards ("HIPAA Security Rule").[150] HIPAA applies to health plans,[151] health care clearinghouses,[152] and health care providers that transmit health information in electronic form.[153]

The Transactions Rule created standards for electronic transactions and the data elements[154] included in electronic transactions to facilitate the electronic exchange of health care information.[155] The Transactions Rule requires all covered companies to update their computer systems to meet the rule.[156] Implementing new uniform standards should improve the utility of the health care system, reduce administration costs, and force companies to re-evaluate the security systems currently in use.[157]

The HIPAA Privacy Rule provides standards to assure that "protected health information"[158] is properly protected by "covered entities."[159] The HIPAA Privacy Rule requires "covered entities" to provide privacy notices,[160] establish appropriate safeguards,[161] and provide staff training.[162] It also requires companies to limit disclosures by making efforts to use, disclose, and request only the minimum amount of protected health information needed to fulfill the purpose of the disclosure.[163] A covered entity can use protected health information only

147. 42 U.S.C. § 1320(d)(6) (2006). "Individually identifiable health information" is any information that "(A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (B) relates to the past present or future physical or mental health or condition of an individual, the provision of health care to an individual, and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual." *Id.*

148. 45 C.F.R. §§ 160, 162 (2006).

149. *See* 45 C.F.R. §§ 160, 164 (2006).

150. *See* 45 C.F.R. §§ 160, 162, 164 (2006).

151. Pub. L. No. 104-191 § 1172(a)(1).

152. *Id.* § 1172(a)(2).

153. *Id.* § 1172(a)(3).

154. 45 C.F.R. § 160.103 (2006). A "data element" is "the smallest named unit of information in a transaction." *Id.*

155. *See* 42 U.S.C. § 1320d-2(a).

156. *See* 45 C.F.R. § 163.923(a) (2006).

157. WESTBY, PRIVACY, *supra* note 67, at 40.

158. "Protected health information" is "individually identifiable health information" that is transmitted or maintained using electronic media. 45 C.F.R. § 164.501.

159. "Covered entities" are health plans, health care clearinghouses, and health care providers. *Id.* § 160.103.

160. *Id.* § 164.520.

161. *See id.* § 164.530(c).

162. *Id.* § 164.530(b).

163. *Id.* § 164.502(b).

as the HIPAA Privacy Rule permits or with written authorization by the individual who the information is about.[164] However, the HIPAA Privacy Rule does not restrict the use or disclosure of "de-identified health information."[165]

The HIPAA Privacy Rule also permits the disclosure and use of protected health information without an individual's authorization in some situations where the information is not de-identified.[166] A covered entity can disclose protected health information directly to the individual.[167] Protected health information can be used and disclosed by a covered entity for its own treatment, payment and health care operations activities.[168] Information can be disclosed by obtaining the owner's oral consent or in situations where the individual clearly has the opportunity to agree or object to the disclosure and does not.[169] Disclosures can also be made where public health protection,[170] law enforcement,[171] and worker's compensation determinations[172] require.

The HIPAA Privacy Rule does take several measures to limit the amount of information that is disclosed to that which is necessary[173] and to make sure that consumers are aware of the privacy policies of the companies with which they are dealing.[174] The rule requires companies to implement "minimum necessary" policies that limit the employees who have access to protected information,[175] and limit the amount of information disclosed to that which is reasonably necessary to carry out the purpose of the request.[176] Companies also must implement reasonable technical, administrative, and physical safeguards to maintain the privacy of protected information.[177] While these standards do force organizations to look seriously at their data security systems, they are not overly burdensome[178] because the rule provides exceptions and only

164. 45 C.F.R. § 164.502(a) (2006).

165. *Id.* § 164.502(d)(2). Health information that does not identify or provide a reasonable method for identifying an individual is "de-identified." *Id.* § 164.514(a).

166. *Id.* § 164.502(a)(1).

167. *See id.* § 164.506.

168. *See* 45 C.F.R. § 164.506 (2006).

169. *Id.* § 164.510.

170. *Id.* § 164.512(b).

171. *Id.* § 164.512(f).

172. *Id.* § 164.512(l).

173. *See* 45 C.F.R. § 164.502(b) (2006).

174. *Id.* § 164.520(a)-(b).

175. *Id.* § 164.514(d)(2).

176. *Id.* § 164.514(d)(3).

177. *Id.* § 164.530(c).

178. *See supra* notes 165-72 and accompanying text. The Privacy Rule also creates another exception under which protected information can be disclosed. A disclosure that is incidental to or occurs as a by-product of another disclosure is permitted as long as the company has applied reasonable safeguards and the minimum necessary standards. *See*

requires a company to "reasonably safeguard" information.[179]

Privacy cannot be achieved without appropriate information security.[180] The HIPAA Security Rule[181] supports the HIPAA Privacy Rule by providing "standards, implementation specifications, and requirements . . . with respect to electronic protected health information."[182] Covered entities must ensure the confidentiality, integrity, and availability of electronically protected health information, protect against anticipated security and integrity threats, protect against non-permitted disclosures, and ensure compliance by employees.[183] To achieve these goals, a covered entity is permitted to use "any security measure . . . [that] reasonably and appropriately implement[s]" these standards.[184] While this approach is flexible, the rule requires that an organization consider several factors when it determines what security measures to implement.[185] Considerations include the entity's size, complexity, and capabilities;[186] the entity's technical infrastructure, hardware, and software capabilities;[187] the cost of proposed security measures;[188] and the probability of potential risks.[189]

In addition to these guidelines, the HIPAA Security Rule provides more detailed requirements related to administrative safeguards,[190] physical safeguards,[191] technical safeguards,[192] organizational requirements,[193] and documentation.[194] These implementation specifications are divided into two categories: "required" and "addressable."[195] A covered entity must implement "required" specifications.[196] While "addressable" specifications must be considered by all covered entities, their implementation is only required in specific

---

id. § 164.502.

179. *See id.* § 164.530(c)(2).

180. *See* WESTBY, SECURITY, *supra* note 67, at 19 (privacy of data is directly dependent upon security).

181. Covered entities were required to be in compliance with the HIPAA Security Rule by April 20, 2005. 45 C.F.R. § 164.318 (2006).

182. *Id.* § 164.302.

183. *Id.* § 164.306(a).

184. *Id.* § 164.306(b)(1).

185. *Id.* § 164.306(b)(2).

186. 45 C.F.R. § 164.306(b)(2)(i) (2006).

187. *Id.* § 164.306(b)(2)(ii).

188. *Id.* § 164.306(b)(2)(iii).

189. *Id.* § 164.306(b)(2)(iv).

190. *Id.* § 164.308.

191. 45 C.F.R. § 164.310 (2006).

192. *Id.* § 164.312.

193. *Id.* § 164.314.

194. *Id.* § 164.308.

195. Each implementation specification is labeled either "required" or "addressable" following the title of each specification. *Id.* § 164.306(d)(1).

196. 45 C.F.R. § 164.306(d)(2) (2006).

situations.[197] A company must access each "addressable" specification in the context of its organization and determine if the specification is a "reasonable and appropriate safeguard."[198] Each "addressable" specification that is applicable to the entity must be implemented if it is "reasonable and appropriate."[199] If a company finds that an "addressable" specification is not "reasonable and appropriate," it must justify and document its findings and implement a "reasonable and appropriate" alternative if one exists.[200]

Obligatory administrative safeguards call for a covered entity to implement a security management process to "prevent, detect, contain, and correct security violations."[201] Four "required" implementation specifications address this goal: a risk analysis assessment, a risk management program, a policy to sanction employees who do not comply with the company's security policies, and a regular review of information system activity.[202] A covered entity must assign responsibility for security to a security official.[203] The implementation of policies and procedures to make sure that employees have appropriate access to protected information is dealt with through "addressable" specifications.[204] Covered entities should implement an employee security awareness and training program[205] and procedures to deal with security incidents.[206] The administrative safeguards also call for a contingency plan that allows the company to recover its systems without damage to data in the event of a natural disaster or system failure.[207] The changing technical environment is addressed as well; a covered entity must perform "periodic technical and nontechincal evaluation[s]."[208]

The physical safeguards of the HIPAA Security rule address the physical machines used to process and store data, as well as the buildings in which these machines reside.[209] A covered entity must implement

197. *See id.* § 164.306(d)(3).
198. *Id.* § 164.306(d)(3)(i).
199. *Id.* § 164.306(d)(3)(ii)(A).
200. *Id.* § 164.306(d)(3)(ii)(B).
201. 45 C.F.R. § 164.308(a)(1)(i) (2006).
202. *Id.* §§ 164.308(a)(1)(ii)(A)-(D). Records containing information system activity includes "audit logs, access reports, and security incident tracking reports." *Id.* § 164.308(a)(1)(ii)(D).
203. *Id.* § 164.308(a)(2).
204. *Id.* § 164.308(a)(3)(ii).
205. *Id.* § 164.308(a)(5)(i). "Addressable" implementation specifications that advance the goal of an effective employee training and awareness program are security reminders and updates, procedures for guarding against malicious software, monitoring system log-ins, and password management procedures. *Id.* §§ 164.308(a)(5)(ii)(A)-(D).
206. 45 C.F.R. § 164.308(a)(6)(i) (2006).
207. *See id.* §§ 164.308(a)(7)(i)-(ii).
208. *Id.* § 164.308(a)(8).
209. *See id.* § 164.310.

policies and procedures to limit access to systems containing protected information.[210] "Addressable" implementation specifications include creating procedures to control access to facilities, control access to software, and safeguard a company's physical machines.[211] Finally, policies and procedures must be developed to deal with the movement, re-use, and disposition of any physical hardware containing protected information.[212]

The technical safeguards of the HIPAA Security Rule address access to electronic data and the transmission of protected data.[213] A covered entity has to implement policies to restrict access to protected health information by individuals and software programs.[214] These policies must include unique user identification for the purpose of tracking users,[215] a method for accessing information during an emergency, automatic system logoff, and mechanisms to encrypt protected information.[216] The technology safeguards also provide for security measures during the transmission of data over an electronic network.[217] Two "addressable" implementation standards call for companies to ensure data integrity and to encrypt protected information in appropriate circumstances.[218]

The HIPAA Security Rule holds an organization responsible for the actions of its business associates by requiring that any contract with a business associate include provisions that require the business associate to protect any private health information obtained from the covered entity.[219] The HIPAA Security Rule's documentation requirements help make sure that the organization considers and attends to the requirements of the rule.[220] A written record of the actions, activities, and assessments

210. *See id.* § 164.310(a).

211. 45 C.F.R. § 164.310(a)(2) (2006).

212. *Id.* §§ 164.310(d)(1)-(2). An "addressable" implementation specification also requires that all electronically protected health information is backed-up before any physical equipment is moved. *Id.* § 164.310(d)(2)(iv).

213. *See id.* § 164.312.

214. *Id.* § 164.312(a)(1).

215. *See id.* § 164.312(b). Unique user ID's allow the implementation of audit controls for the purpose of recording activity in information systems that contain protected data. *Id.* Procedures to verify that a person seeking access to protected data is authorized help ensure that the audit controls are accurate. *See id.* § 164.312(c).

216. 45 C.F.R. § 164.312(a)(2) (2006).

217. *Id.* § 164.312(e)(1).

218. *Id.* § 164.312(e)(2).

219. *See id.* § 164.314.

220. *See id.* §§ 164.316(b)(2)(ii) (requiring that documentation be made available for individuals responsible for implementing necessary procedures) and 164.316(b)(2)(iii) (requiring that documentation be reviewed and updated as "environmental or operational changes affecting the security of electronic protected health information" demand).

required by the rule must be retained by an organization for six years.[221]

The HIPAA Privacy Rule and HIPAA Security Rule provide detailed requirements, while acknowledging that flexibility is necessary based on each organization's size, function, and unique characteristics.[222] When an organization does disclose protected health information it must use reasonable efforts to disclose only the minimum amount of information necessary under the circumstances.[223] The HIPAA Security Rule offers protection for electronic health information by providing implementation specifications that must be put in place.[224] HIPAA's requirements are given weight through a number of criminal and civil penalties.[225] Some argue that the specific requirements of the HIPAA Security Rule combined with the potential for criminal penalties might be too much too soon.[226] The cost of compliance may have an impact on covered organizations, adversely affecting the quality of health care.[227] While the Security Rules are extensive, they do allow a covered entity the flexibility to implement their requirements in a manner that is appropriate to the individual organization.[228]

C. *Federal Information Security Management Act ("FISMA")*

The Federal Information Security Management Act of 2002 ("FISMA") provides the framework for the information security[229] of

---

221. 45 C.F.R. § 164.316(b)(2)(i).

222. *See id.* §§ 160, 162, 164.

223. *Id.* § 164.502(b).

224. *Id.* § 164.302. *See also id.* §§ 164.306, 164.308, 164.310, and 164.312.

225. *See* 42 U.S.C. §§ 1176-77 (2006).

226. WESTBY, PRIVACY, *supra* note 67, at 44 (arguing that the HIPAA Security Rules cause confusion and suggesting that government regulators need to better understand cyber security before enacting regulations of this type).

227. *See id.* at 46.

228. *See, e.g.*, 45 C.F.R. §§ 164.306(b)(2) (2006) (allowing the following factors to be considered in determining which security measures to use: size, complexity, and capabilities of the covered entity, technical infrastructure, including hardware and software capabilities, cost, the probability of potential risks); 164.306(d)(3)(ii)(B) ("addressable implementation specifications only need to be implemented if "reasonable and appropriate"); 164.312(e)(2)(ii) (a mechanism must be implemented "to encrypt electronic protected health information *whenever deemed appropriate*") (emphasis added).

229. FISMA comprehensively defines "information security:"

> The term "Information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide–
>
> (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
>
> (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and

federal information systems.[230] The Director of the Office of Management and Budget ("Director")[231] oversees information security policies for all agencies.[232] The Director must require federal agencies to identify and provide information security that is appropriate for the "risk and magnitude of harm [that would result] from the unauthorized access, use, disclosure, disruption, modification, or destruction of" information gathered by the agency and information systems used by the agency.[233] The Director also must review the agencies' information security programs at least annually.[234] While the Director is responsible for coordinating the information security policies of all federal agencies,[235] each agency is responsible for implementing an information security policy that best fits its own needs.[236]

Each agency must conduct a risk assessment,[237] determine the level of security necessary to protect its information and information systems,[238] implement cost-effective methods to reduce these risks,[239] and periodically test its systems to make sure the methods are effective.[240] FISMA authorizes the designation of a senior agency information security officer.[241] This officer has to "possess professional qualifications" and has one primary duty: information security.[242]

Compliance with FISMA is monitored in several ways. First, each agency is required to perform an independent evaluation of its security program.[243] The evaluation must test the effectiveness of the agency's policies and procedures and assess the agency's compliance with FISMA.[244] Each agency is required to report the results of its evaluation to the Director.[245]

FISMA seems to offer strong tools that encourage agencies to

---

proprietary information ; and
(C) availability, which means ensuring timely and reliable access to and use of information.

44 U.S.C. § 3542(b)(1).

230. *See id.* § 3541.
231. *Id.* § 3502(4).
232. *Id.* § 3543(a).
233. *Id.* § 3543(a)(2).
234. 44 U.S.C. § 3543(a)(5).
235. *Id.* § 3543(a)(6).
236. *See id.* § 3544.
237. *Id.* § 3544(a)(2)(A).
238. *Id.* § 3544(a)(2)(B).
239. 44 U.S.C. § 3544(a)(2)(C).
240. *Id.* § 3544(a)(2)(D).
241. *Id.* § 3544(a)(3).
242. *Id.* §§ 3544(a)(3)(A)(ii)-(iii).
243. *Id.* § 3545(a)(1).
244. 44 U.S.C. § 3545(a)(2)(A)-(B).
245. *Id.* § 3545(e)(1).

implement successful security procedures.[246] Agencies are held accountable by the evaluation and reporting requirements.[247] Unfortunately, the most recent results of these evaluations reveal weaknesses.[248] An assessment of how well agencies met the requirements of FISMA left the federal government with an overall grade of "D+" and seven agencies[249] with failing scores for their data security efforts.[250] While the government's overall grade was an improvement over the previous year's "D," other evidence suggests that federal agencies are failing in their efforts to comply with FISMA.[251]

IV. Data Not Currently Protected by Specific Legislation: The FTC Cracks Down on "Deceptive Trade Practices"

A. FTC Consent Decrees

Even before the recent media coverage of identity theft, the FTC used its authority to prevent unfair or deceptive trade practices under the FTC Act[252] to make sure that companies kept the data security promises they made to consumers.[253] The FTC has filed complaints against several companies that failed to take precautions to secure their customers' information as promised in their online privacy policies.[254] The FTC has also used its power to prevent unfair practices to challenge

246. *See, e.g., id.* § 3544(a)(3) (calling for the appointment of a senior agency information security officer).

247. *See, e.g., id.* § 3545(a)(1) (requiring independent evaluation of each agency's security program); 44 U.S.C. § 3545(e)(1) (requiring yearly reporting of evaluations to the Director).

248. *See* Nikki Swartz, *Cybersecurity Report Reveals Weaknesses.* 39 INFO. MGMT. J. 19, 19 (2005) [hereinafter *Cybersecurity Report*] (at least half of all U.S. federal agencies received a grade of "D" or worse on the House Government Reform Committee's annual report).

249. The departments of Agriculture, Commerce, Energy, Health and Human Services, Housing and Urban Development, Homeland Security, and Veterans Affairs all received failing grades for the year 2004. The departments of Defense and Treasury, as well as the National Aeronautics and Space Administration and the Small Business Administration were not far behind, each receiving a grade of "D." *Id.*

250. *Id.*

251. *See, e.g., id.* (while ten agencies improved their grades from 2003, eight others received lower marks than they did in 2003); Joanie Wexler, *Federal agencies need to improve Wi-Fi controls; *NIST to develop updated wireless guidelines,* NETWORK WORLD, July 6, 2005 (suggesting few agencies have implemented appropriate security measures).

252. 15 U.S.C. §§ 41-58 (2006).

253. FTC Privacy Initiatives, *supra* note 18.

254. *E.g., In re* Guess?, Inc., No. C-4091, 2003 FTC LEXIS 123 (July 30, 2003), *available at* http://www.ftc.gov/ os/2003/08/guessdo.pdf.

information security practices that cause consumer injury.[255] The FTC has entered consent agreements with many of the companies it has filed complaints against (collectively "FTC Consent Orders").[256] These agreements outline a consistent standard that offending companies must meet and offer guidance about what must be done to avoid liability for failing to protect consumer data.[257]

1. BJ's Wholesale Club

The FTC alleged that BJ's Wholesale Club ("BJ's") did not employ reasonable standards to secure data collected from customers at its stores from at least November 1, 2003 until February, 2004.[258] Subsequently, BJ's entered into a consent order with the FTC ("BJ's Order") to resolve these allegations.[259] According to the FTC, BJ's (1) did not encrypt information while in transit or while stored on in-store computer networks, (2) stored information in files that could be accessed using a known default user ID and password, (3) did not use available security measures to secure wireless access points on its networks, (4) did not conduct security investigations, and (5) put data at risk by storing it for up to thirty days after it had a business need to keep the information.[260]

BJ's used computer networks to obtain authorization for credit card and debit card purchases.[261] In order to authenticate a customer's card, BJ's collected personal information[262] from the magnetic strip on the

255. *See, e.g., id.*

256. *Id.; In re* Eli Lilly & Co., No. C-4047, 2002 FTC LEXIS 22 (May 8, 2002), *available at* http://www.ftc.gov/os/2002/05/elililly do.htm; *In re* BJ's Wholesale Club, Inc., No. C-4148, 2005 FTC LEXIS 134 (Sept. 20, 2005), *available at* http://www.ftc.gov/os/caselist/0423160/092305do0423160.pdf.

257. *See, e.g., In re* Eli Lilly & Co., No. C-4047, 2002 FTC LEXIS 22 (May 8, 2002), *available at* http://www.ftc.gov/os/2002/05/elililly do.htm.

258. Complaint at 3, *In re* BJ's Wholesale Club, Inc., No. C-4148, 2005 FTC LEXIS 134 (Sept. 20, 2005), *available at* http://www.ftc.gov/os/caselist/0423160/092305comp 0423160.pdf.

259. *In re* BJ's Wholesale Club, Inc., 2005 FTC LEXIS 134.

260. Complaint at 2, *In re* BJ's Wholesale Club, Inc., 2005 FTC LEXIS 134.

261. *Id.*

262. "Personal information" was defined in the BJ's Order to include but not be limited to

> (a) first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identification or a screen name that reveals an individual's email address; (d) a telephone number; (e) a Social Security number; (f) credit and/or debit card information, including credit and/or debit card number, expiration date, and data stored on the magnetic stripe of a credit or debit card; (g) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual consumer; or (h) any other information from or about an individual consumer that is combined with (a)

customer's credit or debit card.[263] After the information from the card's magnetic strip was collected, it was used to form an authorization request.[264] That request was transmitted from the in-store network to BJ's central datacenter.[265] From there, outside networks transferred the request to the card's issuing bank.[266] The issuing bank then granted or denied the request through the same networks.[267] BJ's also used wireless scanners to manage inventory.[268] The FTC alleged that a hacker could use the wireless access points connecting the scanners to the network to access BJ's network and steal personal information.[269]

Several customers who used their cards at BJ's stores discovered that fraudulent purchases were made using copies of the information on their cards.[270] The FTC alleged that information that was stored on BJ's network was stolen and used to make counterfeit cards.[271] The customers and their banks had to cancel and reissue thousands of credit cards.[272] During this process, several customers were unable to access their bank accounts.[273]

The BJ's Order[274] required BJ's to "implement and . . . maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers."[275] At a minimum, BJ's information security program must include a designated program coordinator, a risk assessment, and the implementation of reasonable safeguards based on the risk assessment.[276] The risk assessment should consider, at a minimum, employee training and management, network and software design, information processing, data storage, data

---

and (g) above.

In re BJ's Wholesale Club, Inc., 2005 FTC LEXIS 134, at *2-3.

263. Complaint at 3, *In re* BJ's Wholesale Club, Inc., 2005 FTC LEXIS 134 (Sept. 20, 2005).

264. *Id.* at 2.

265. *Id.*

266. *Id.*

267. *Id.*

268. *In re BJ's Wholesale Club, Inc.*, 2005 FTC LEXIS 134 at *2.

269. *Id.*

270. *Id.*

271. *Id.*

272. *Id.*

273. *In re BJ's Wholesale Club, Inc.*, 2005 FTC LEXIS 134 at *2.

274. The terms of the agreement provide that BJ's entered it for "settlement purposes only" and the agreement does not serve as an admission to anything contained in the FTC's complaint. *In re* BJ's Wholesale Club, Inc., No. C-4148, 2005 FTC LEXIS 134, at *1 (Sept. 20, 2005), *available at* http://www.ftc.gov/os/caselist/0423160/092305do0423160.pdf.

275. *Id.* at *4.

276. *Id.* at *4-5.

transmission, and procedures to prevent, detect, and respond to attacks.[277] Furthermore, BJ's has to provide a third-party[278] assessment and report to the FTC biennially for twenty years.[279] The third-party report must describe what safeguards BJ's set forth, why they are appropriate based on characteristics[280] unique to BJ's business, and how they meet or exceed the protections required by the BJ's Order.[281] The terms of the BJ's Order, issued on May 17, 2005, do not terminate for twenty years.[282]

2. Eli Lilly

In 2002, the FTC entered a consent agreement ("Eli Lilly Order") with Eli Lilly and Company ("Eli Lilly"), a pharmaceutical company.[283] The FTC alleged that Eli Lilly misrepresented the protection it offered for consumers' personally identifiable information.[284] Eli Lilly promoted Prozac through two company websites.[285] As part of the Prozac marketing campaign, Eli Lilly offered a service called "Medi-messenger."[286] This reminder service allowed consumers to design and receive personal email reminders about their medication from Eli Lilly.[287] In order to use this service, a consumer simply had to register for it by providing an email address, a password, and a schedule of the dates he or she wished to receive reminders.[288]

After the consumer provided the required information, he or she had the option to view the web site's "Privacy Statement" by clicking a hyperlink.[289] The "Privacy Statement" contained several provisions either expressly stating or implying that Eli Lilly employed appropriate

277. *Id.* at *5.

278. The third party must be qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); hold a Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or be otherwise qualified and approved by the FTC. *Id.* at *6-7.

279. *In re BJ's Wholesale Club, Inc.*, 2005 FTC LEXIS 134 at *5-6.

280. The safeguards must be appropriate in light of BJ's size and complexity, the nature and scope of BJ's activities, and the sensitivity of the information it collects. *Id.* at *4.

281. *Id.* at *6.

282. *Id.* at *10. The order will be extended if the FTC files a complaint alleging a violation of the order in federal court. *Id.*

283. *In re* Eli Lilly & Co., No. C-4047, 2002 FTC LEXIS 22 (May 8, 2002), *available at* http://www.ftc.gov/os/2002/05/elililly do.htm.

284. Complaint at *1, *In re* Eli Lilly & Co., No. C-4047, 2002 FTC LEXIS 22 (May 8, 2002), *available at* http://www.ftc.gov/os/2002/05/elililly cmp.htm.

285. *Id.*

286. *Id.*

287. *Id.* at *2.

288. *In re Eli Lilly & Co.*, 2002 FTC LEXIS 22 at *2.

289. *Id.*

steps to protect the privacy and confidentiality of personal information obtained from consumers.[290] On June 27, 2001, Eli Lilly decided to discontinue the "Medi-messenger" service.[291] An Eli Lilly employee created a computer program to access the email addresses of the "Medi-messenger" participants and alert them of the service's discontinuation.[292] The new computer program generated an email and sent it to all of the "Medi-messenger" subscribers.[293] The email included all the recipients' email addresses in the "To:" line.[294] The FTC alleged that Eli Lilly could have prevented the disclosure of these 669 "Medi-messenger" users' personal information if it had implemented and maintained "internal measures appropriate under the circumstances."[295]

While the FTC's complaint suggests that Eli Lilly's failure to take "appropriate" measures was contrary to its "Privacy Statement," it is unclear whether Eli Lilly's failure to maintain "appropriate security" measures would have generated FTC action in the absence of the representations made in the "Privacy Statement."[296] It is clear that the Eli Lilly Order addresses Eli Lilly's future actions in both areas. Eli Lilly "shall not misrepresent . . . expressly or by implication, the extent to which it maintains and protects the privacy or confidentiality of any personally identifiable information collected from or about consumers. . . ."[297] The Eli Lilly Order also required Eli Lilly to establish and maintain an information security program.[298] This program had to include a designated employee to oversee it, a risk management assessment, and an annual written review.[299] The Eli Lilly Order

290. *Id.* at *2-4. The "Privacy Statement included the following statements: "Eli Lilly . . . respects the privacy of visitors to its Web sites, and we feel it is important to maintain our guests' privacy as they take advantage of this resource" and "[Our] security measures help us to honor your choices for the use of Your Information." *Id.*

291. *Id.* at *5.

292. *Id.*

293. *Id.*

294. *In re Eli Lilly & Co.*, 2002 FTC LEXIS 22 at *5.

295. *Id.* at *5-6. The FTC alleged that Eli Lilly did not provide training for its employees about consumer privacy and information safety, and did not provide appropriate training and supervision for the employee who sent the email. *Id.* The employee was inexperienced with the computer program that was used. *Id.* Additionally, the FTC alleged that Eli Lilly failed to use appropriate testing and control processes before allowing the email to be sent. *See id.*

296. *See id.* at *6-7 (stating the failure to maintain appropriate standards and the violation of Eli Lilly's own policies as separate counts). *See also In re* Eli Lilly & Co., No. C-4047, 2002 FTC LEXIS 22, at *10-11 (May 8, 2002), *available at* http://www.ftc.gov/os/2002/05/elilillydo.htm (corrective action includes both the proper representation of Eli Lilly's privacy policies and the implementation of appropriate security policies).

297. *In re* Eli Lilly & Company, 2002 FTC LEXIS 22, at *10-11.

298. *Id.* at *11.

299. *Id.* at *10-11.

required the risk management assessment to address three areas: management and training of personnel, physical systems and media, and attack and intrusion prevention.[300]

While the disclosure of a few hundred email addresses may not have had the same financial impact as larger data breaches, the Eli Lilly "Medi-messenger" mistake illustrates the need for a comprehensive information security policy. It is likely that this disclosure could have been prevented if Eli Lilly had exercised proper training, program testing, and management.[301] More importantly, it raises a question regarding the origin of a company's obligations when it comes to security. Are a company's obligations self-imposed like Eli Lilly's "Privacy Statement,"[302] based on external ideas of "adequacy,"[303] or a combination of both?

3. Guess?

The FTC entered into a consent agreement ("Guess Order") with Guess?, Inc. and Guess.com, Inc. ("Guess") in 2003.[304] Guess designs and sells clothing. In addition to selling products in its own stores and through independent retailers, Guess also sells clothing through its website.[305] Like the allegations against Eli Lilly, the allegations against Guess included both misrepresentations of Guess's privacy policy and failures to use appropriate measures to secure personal information.[306] In order to facilitate online purchases, Guess required consumers to provide their credit card numbers and other personal information.[307]

The FTC alleged that Guess stored the information it collected in

300. *Id.* at *10.

301. *See* Complaint at *5-6, In re Eli Lilly & Co., No. C-4047, 2002 FTC LEXIS 22 (May 8, 2002), *available at* http://www.ftc.gov/os/2002/05/elilillycmp.htm (program was written by an inexperienced employee and not tested before being used).

302. *See, e.g., In re* Gateway Learning Co., No. C-4120, 2004 FTC LEXIS 150 (Sept. 10, 2004), *available at* http://www.ftc.gov/os/caselist/0423047/040917comp0423047.pdf (allegations against Gateway arose when Gateway changed its privacy policy to permit third-party sharing of personal information without alerting consumers). This was the first FTC case to challenge deceptive practices in connection with a company making a change to its privacy policy. *See id.*

303. *See In re* BJ's Wholesale Club, Inc., No. C-4148, 2005 FTC LEXIS 134, at *3-5 (Sept. 20, 2005), *available at* http://www.ftc.gov/os/caselist/0423160/092305do0423160.pdf.

304. *In re* Guess?, Inc., No. C-4091, 2003 FTC LEXIS 123 (July 30, 2003), *available at* http://www.ftc.gov/os/2003/08/guessdo.pdf.

305. Complaint at *1, *In re* Guess?, Inc., No. C-4091, 2003 FTC LEXIS 123, (July 30, 2003), *available at* http://www.ftc.gov/os/2003/08/guesscomp.pdf.

306. *Id.* at *6-7 (suggesting failure to use appropriate security measures caused statements made in privacy policy to be false).

307. *Id.* at *2.

database tables.[308] Customers used a web application[309] to connect to these tables.[310] The application was designed to retrieve information from the database tables and present it on a webpage in clear, readable text.[311] According to the FTC's complaint, Guess also provided a privacy policy on its website.[312] It promised that "all . . . personal information . . . [is] stored in an unreadable encrypted format at all times" and "all user information is further protected by a multi-layer firewall based security system."[313]

According to the FTC, Guess's systems were not as secure as the privacy agreement indicated and were susceptible to "commonly known . . . attacks."[314] The FTC alleged that Guess's databases were vulnerable to attacks such as SQL[315] injection attacks.[316] A hacker using an SQL injection attack enters code in the address bar of a web browser to direct the application to obtain, alter, or delete information stored in the database.[317] The FTC alleged that in February, 2002, someone used an SQL injection attack to read and delete credit card information in one of Guess's databases.[318]

The Guess Order, like the Eli Lilly Order, addressed both Guess's failure to use appropriate security measures and misrepresentations in Guess's privacy policy.[319] Like the Eli Lilly Order, the Guess Order required that Guess establish and maintain a written security program designed to "protect the security, confidentiality, and integrity of personal information collected from or about consumers."[320] The security program must contain administrative, technical and physical safeguards[321] appropriate to Guess's size and business activities.[322] In

308. *Id.*

309. A web application is a software program that is executed by a web server to respond to a request sent from the browser. GREG RICCARDI, DATABASE MANAGEMENT WITH WEB SITE DEVELOPMENT APPLICATION 3 (2003).

310. Complaint at *2-3, *In re* Guess?, Inc., 2003 FTC LEXIS 123.

311. *Id.* at *3.

312. *Id.* at *3-4.

313. *Id.* at *3.

314. *Id.* at *5.

315. SQL or "Structured Query Language" is a standard language for defining the structure of relational databases and manipulating their contents. RICCARDI, *supra* note 309, at 16.

316. Complaint at *5, *In re* Guess?, Inc., 2003 FTC LEXIS 123.

317. *Id.*

318. *Id.* at *6.

319. *In re* Guess?, Inc., No. C-4091, 2003 FTC LEXIS 123, at *11-12 (July 30, 2003), *available at* http://www.ftc.gov/os/2003/08/guessdo.pdf.

320. *Id.* at *12.

321. *Id.* at *12-13. Like the Eli Lilly Order, the Guess Order requires these safeguards, at minimum, to include: a designated coordinator of the information security program, a risk assessment, testing and design of safeguards based on the results of the risk assessment, and evaluation and retesting when changes occur to Guess's business.

addition to requiring the development of a security program, the Guess Order also prohibits Guess from making misrepresentations about how it maintains and protects its customers' privacy.[323] Like the BJ's Order, the Guess Order requires third-party investigations every two years and terminates twenty years from the date it was issued.[324]

B. *How the FTC's "Crackdown" Stacks Up: What a Corporation Can Learn from the FTC Consent Orders*

The FTC Consent Orders make it clear that a company must deliver on the promises it makes to consumers about the way it will protect their personal information.[325] However, the BJ's Order also suggests that even a company that does not make any explicit promises to consumers must maintain adequate security appropriate to its business.[326] While the FTC Consent Orders extend twenty years from the date they are entered, they do acknowledge that security concerns relating to technology are dynamic and business-specific.[327] Hopefully the flexible language of the FTC Consent Orders will allow them to provide effective protection during their long enforcement period even as technology changes. Even though FTC Consent Orders apply to individual companies, they illustrate three areas of concern for any company dealing with personal consumer data.

First, a company dealing with personal information must take its privacy policy seriously.[328] While the BJ's Order was based solely on BJ's failure to implement effective security measures, the other FTC Consent Orders were, at least partially, based on misrepresentations in each company's security policy, created as a result of data security

---

Id.

322. *Id.* at *12.

323. *Id.* at *11.

324. *In re* Guess?, 2003 FTC LEXIS 123, at *13, *18-19. *See also In re* BJ's Wholesale Club, Inc., No. C-4148, 2005 FTC LEXIS 134, at *5-7, *10 (Sept. 20, 2005), *available at* http://www.ftc.gov/os/caselist/0423160/092305do0423160.pdf; *In re* Guess?, Inc., No. C-4091, 2003 FTC LEXIS 123, (July 30, 2003), *available at* http://www.ftc.gov/os/2003/08/guessdo.pdf.

325. *See, e.g., In re* Guess?, Inc., 2003 FTC LEXIS 123.

326. *See In re* BJ's Wholesale Club, Inc., 2005 FTC LEXIS 134.

327. *See, e.g., id.* (stating that the required information security program must contain safeguards "appropriate to [BJ's] size and complexity, the nature and scope of [BJ's] activities, and the sensitivity of the personal information . . ." and "evaluation and adjustment of [BJ's] security program is required based on periodic risk assessments, changes in BJ's business or other circumstances that [BJ's] knows or has reason to know may have a material impact on the effectiveness of its information security program").

328. *See, e.g., In re* Guess?, Inc., 2003 FTC LEXIS 123, at *11 ("[the company] shall not misrepresent . . . the extent to which [it] maintain[s] and protect[s] security, confidentially, or integrity of any personal information").

failures.[329] A company should write an effective privacy policy, make sure that it takes the measures the policy claims, and avoid making material changes to the privacy policy without alerting consumers.[330] On the other hand, a company should not water down its privacy policy in an attempt to avoid liability. The FTC has also used its power to prevent unfair trade practices to take action against companies that fail to take reasonable and appropriate measures to secure data in cases not involving promises in a privacy policy.[331] However, it is very clear that the FTC will hold companies liable for failing to deliver on promises made to consumers in their privacy policies.[332] Therefore, a company should carefully consider whether it can deliver on a promise before including it in its privacy policy.

Second, a company dealing with personal information should create a written, comprehensive, company-wide security program.[333] The security plan should be a strategic document, created at an organizational level, that includes considerations unique to each individual business.[334] The plan should be designed to protect the confidentiality, security, and integrity of personal data.[335] Technical, administrative, and physical safeguards should be identified and implemented as part of a security plan.[336] While the consequences of ineffective security demand that a company design its security plan from a company-wide perspective, an individual employee should be appointed and empowered to coordinate the plan.[337] At a minimum, the safeguards that are implemented as part of a company's security plan should address employee training, employee management, network and software design, data storage and transmission, and intrusion prevention, detection, and response.[338]

Third, a company that collects or uses its customers' personal information should evaluate its information security policies frequently,

329. *E.g., In re* Eli Lilly & Co., No. C-4047, 2002 FTC LEXIS 22 (May 8, 2002), *available at* http://www.ftc.gov/os/2002/05/elilillydo.htm.

330. *See* Complaint at *5-8, *In re* Gateway Learning Co., No. C-4120, 2004 FTC LEXIS 150 (Sept. 10, 2004), *available at* http://www.ftc.gov/os/caselist/0423047/040917comp0423047.pdf (suggesting allegations arose of out changes made to Gateway's privacy policy allowing the company to share information when the policy previously promised that data would not be shared with outside sources).

331. *See*, e.g., *In re* BJ's Wholesale Club, Inc., No. C-4148, 2005 FTC LEXIS 134 (Sept. 20, 2005), *available at* http://www.ftc.gov/os/caselist/0423160/092305comp0423160.pdf.

332. *E.g., In re* Eli Lilly & Co., 2002 FTC LEXIS 22.

333. *E.g., In re* MTS, Inc., C-4110, 2004 FTC LEXIS 88, at *11-12 (May 28, 2004), *available at* http://www.ftc.gov/os/caselist/0423047/040917do0423047.pdf.

334. See WESTBY, SECURITY, *supra* note 67, at 187.

335. *E.g., In re* MTS, Inc., 2004 FTC LEXIS 88, at *12.

336. *See, e.g., id.*

337. *See, e.g., id.*

338. *See, e.g., id.* at *12-13.

using both internal and external auditing methods.[339] At a minimum, a company should reevaluate its security plan when it makes a change to its operations or business processes.[340] As Howard Beales, the Director of the FTC's Bureau of Consumer Protection said, "change is inevitable [but] . . . [c]ompanies must . . . make sure . . . changes do not create new vulnerabilities."[341] How often a company should conduct external audits is a question unique to a company's individual business needs. However, any company dealing with its customers' personal information should obtain an outside audit conducted by a qualified[342] person at least every two years.[343] Frequent audits not only can save a company the embarrassment and expense associated with a security incident, but also assure that appropriate industry best practices are being used.[344]

While the FTC Consent Orders provide some guidance for a company that collects its consumers' personal information, some have argued that more should be required. Some argue that a company, which must collect personal information, should collect only the minimum information needed to complete a transaction.[345] The FTC Consent Orders do not prohibit the offending companies from collecting unnecessary data.[346] While the requirement of external audits is generally praised, some argue that two years between audits is too long.[347] Finally, none of the FTC Orders imposed monetary penalties on

339. *See, e.g., In re* BJ's Wholesale Club, Inc., No. C-4148, 2005 FTC LEXIS 134, at *5-6 (Sept. 20, 2005), *available at* http://www.ftc.gov/os/caselist/0423160/092305do0423160.pdf.

340. *E.g., id.* at 5.

341. Press Release, U.S. Fed. Trade Comm'n, Tower Records Settles FTC Charges (Apr. 21, 2004) [hereinafter Tower] *available at* http://www.ftc.gov/opa/2004/04/towerrecords.htm. Mr. Beales went on to compare changes in technical infrastructure to changes in physical infrastructure, saying "Just as [someone who] remodel[ed] their home[] would make sure that the doors still ha[d] locks, companies should make sure that sensitive data is still protected [after a change is made in the company's technical infrastructure]." *Id.*

342. The third party should be qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); hold a Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or be otherwise qualified. *See, e.g., In re* BJ's Wholesale Club, Inc., 2005 FTC LEXIS 134, at *6-7.

343. *See, e.g., id.* at *5-6 (requiring BJ's to obtain an independent report every two years).

344. *See, e.g.,* Bill Hayes, *Conducting a Security Audit: An Introductory Overview,* SECURITY FOCUS, May 26, 2003, http://www.securityfocus.com/print/infocus/1697 (typical information security audit provides measurable ways to correct deficiencies).

345. Letter from Adam Shostack to the FTC (July 5, 2005), http://www.ftc.gov/os/comments/bjswholesaleclub/050715shostack.pdf [hereinafter Shostack Letter] (criticizing the BJ's Order).

346. *See, e.g., In re* BJ's Wholesale Club, Inc., 2005 FTC LEXIS 134.

347. Letter from American Community Bankers to the FTC (July 14, 2005), http://www.ftc.gov/os/comments/bjswholesaleclub/050714amercommunbank.pdf (last

the offending companies.[348] If monetary penalties are not imposed, some question whether companies will aggressively protect consumer information.[349]

C. *Common Law Tort Liability: BJ's Wholesale Club Revisited*

Although the results of electronic fraud and identity theft can be debilitating for individual consumers, often the bank that issued a stolen credit card incurs the costs of the fraudulent transaction.[350] As a result of BJ's failure to properly secure its information systems, its customers' personal information was stolen.[351] Several of the stolen credit card numbers belonged to customers of Sovereign Bank ("Sovereign").[352] Sovereign sued BJ's to recover the cost of replacing the stolen cards with new ones and reimbursing cardholders who were victimized.[353]

Sovereign participates in a system operated by Visa.[354] The Visa system consists of "issuing members," "acquiring members," and "merchants."[355] An "issuing member" issues Visa cards to its customers.[356] An "acquiring member" enters contracts with "merchants" and processes card transactions.[357] A "merchant" allows cardholders to pay for goods or services with a Visa card.[358] In this case, Sovereign was an "issuing member," Fifth Third Bank ("Fifth Third") was an "acquiring member" and BJ's was a "merchant."[359] Fifth Third, as an "acquiring member," contracted[360] with BJ's to process credit card transactions. In

---

visited Nov. 19, 2006) [hereinafter Bankers' Letter] (suggesting that an external audit should be required yearly).

348. *See, e.g.*, *In re* Guess?, Inc., No. C-4091, 2003 FTC LEXIS 123 (July 30, 2003), *available at* http://www.ftc.gov/os/2003/08/guessdo.pdf.

349. *See* Bankers' Letter, *supra* note 347. *But see* FINANCIAL INSTITUTIONS, *supra* note 143 (business incentives independent from legal obligations motivate the protection of customer information).

350. Letter from Visa to the FTC (July 18, 2005), http://www.ftc.gov/os/comments/bjswholesaleclub/050718visa.pdf (Institutions that are Visa members do not impose losses resulting from fraudulent transactions on cardholders.). *See also* Truth in Lending Act, 15 U.S.C. § 1643(a) (2006) (relieves cardholders of any obligation in excess of fifty dollars resulting from the unauthorized use of their card).

351. *See supra* Part IV.A.1.

352. Sovereign Bank v. BJ's Wholesale Club, Inc., 395 F. Supp. 2d 183, 187 (M.D. Pa. 2005).

353. *Id.*

354. *Id.*

355. *Id.* at 189.

356. *Id.*

357. *Sovereign Bank*, 395 F. Supp. 2d at 189.

358. *Id.*

359. *Id.*

360. *Id.* BJ's and Fifth Third entered into two merchant agreements. One governed purchases made with credit cards. The other governed purchases made with debit cards. *Id.* Collectively, the two contracts will be referred to as "BJ's merchant contract" for

order for a business to become a "merchant" of the Visa member association, it must agree to Visa's operating regulations.[361]

The Visa operating regulations prohibit a merchant from storing or retaining cardholder information.[362] Sovereign alleged that BJ's failed to comply with this requirement because the computer program BJ's used to process credit card sales retained card numbers, instead of keeping them in the system only during the validation process.[363] BJ's failure to properly secure its customers' data[364] led to theft of credit card numbers and unauthorized charges.[365] Sovereign sued BJ's[366] on three counts: negligence, breach of contract, and equitable indemnification.[367]

Only the negligence claim survived summary judgment.[368] The court found that BJ's owed Sovereign a duty of care when dealing with its customers' information.[369] A relationship existed between Sovereign and BJ's because both participated in the Visa network.[370] The risk that theft could result from violating the Visa operating agreement was foreseeable; the agreement prohibited a merchant from storing customer data for this very reason.[371] BJ's was in the best position to make sure that data was not stolen by complying with Visa's requirement that data is stored only as long as needed to complete a transaction.[372] Finally, the public benefits from imposing a duty on BJ's in this situation. If merchants are not required to abide by security standards, consumers will lose faith in credit transactions.[373] For these reasons, the court found that BJ's owed the issuing bank a duty of care when processing credit transactions and denied BJ's motion to dismiss.[374]

---

purposes of this discussion.

361. *Id.*

362. *Sovereign Bank*, 395 F. Supp. 2d at 189.

363. *Id.* at 187.

364. *See* discussion *supra* Part IV.A.1.

365. *Sovereign Bank*, 395 F. Supp. 2d at 189-90.

366. Sovereign also sued the "acquiring member," Fifth Third, on the same counts. *Id.* at 190.

367. *Id.*

368. *Id.* The contract claim was dismissed because BJ's negotiated the BJ's merchant contract with Fifth Third, not Sovereign, and the BJ's merchant contract excluded third parties as beneficiaries. *Id.* Sovereign's contract claim against Fifth Third, on the other hand, survived summary judgment because Fifth Third was a party to the contract. *Id.* The equitable indemnification claims against both BJ's and Fifth Third were dismissed because Sovereign failed to establish it had a duty to pay for the unauthorized use of its cards. *Id.* Finally, Sovereign's negligence claim against Fifth Third was dismissed because the court ruled that the economic loss doctrine barred the claim. *Id.*

369. *Id.* at 193.

370. *Sovereign Bank*, 395 F. Supp. 2d at 193.

371. *Id.*

372. *Id.*

373. *See id.*

374. *Id.* at 206.

Although *Sovereign Bank*[375] does suggest that merchants own a duty of care to issuing members when processing consumer credit card purchases, it does not speak to any duty owed directly by a merchant to an individual cardholder. Further, it is unclear whether the economic loss doctrine bars a negligence claim against a merchant. *Sovereign Bank* does not address the economic loss doctrine in relationship to the negligence action against a merchant, but does hold that it prevents recovery from an acquiring member for negligence.[376] However, in *Pennsylvania State Employees Credit Union v. Fifth Third Bank,*[377] another case resulting from BJ's same information security failures, the court held that the economic loss doctrine prevents negligence claims against both the merchant and the acquiring member.[378] Future litigation will determine how broad a merchant's duty to protect personal information is and to whom that duty extends.

V. Analysis and Recommendations

A. All Companies Collecting and Storing Personal Consumer Data Should Develop a Company-Wide Strategy to Secure Electronic Information

Even though information assets often account for the majority of capital spending, few corporate boards understand the importance of information systems and the role IT plays in shaping a company's strategies.[379] While most boards understand and apply established principles in other areas of corporate management,[380] the absence of clear standards in IT governance leaves many Chief Information Officers with the task of managing corporate information assets on their own.[381] No corporation would risk not auditing its books, yet many do not approach IT governance in the same way.[382] The first step in creating an effective

375. 395 F. Supp. 2d 183 (M.D. Pa. 2005).

376. *Id.*

377. 398 F. Supp. 2d 317 (M.D. Pa. 2005).

378. *Id.* at 336 n.16 (stating that Ohio has adopted the economic loss rule). *But see* Banknorth, N.A. v. BJ's Wholesale Club, Inc., 394 F. Supp. 2d 283, 284 (D. Me. 2005) (rejecting a motion to dismiss negligence claims, related to BJ's information security failures, brought against an "acquiring member" and a "merchant").

379. *See* Richard Nolan & F. Warren McFarlan, *Information Technology and the Board of Directors*, HARVARD BUS. REV., Oct. 2005, at 96.

380. Every corporate board is aware, for example, that its corporate accounting practices must comply with Generally Accepted Accounting Principles (GAAP). *Id.* at 98.

381. *Id.*

382. *Id.* It should be noted that some companies are beginning to realize that IT

information security plan is for corporate directors to recognize that IT governance is more than an "IT issue," in the same way that effective corporate accounting is more than an "accounting issue." Both functions are critical to success in today's business environment. Moreover, the failure to recognize that effective management of information security is just as important to a corporation's success as effective accounting practices has consequences paramount to the legal issues inevitably resulting from such failure.[383]

After management seriously commits to IT governance, the company should develop a comprehensive, written information security plan that considers security, privacy, and cybercrime against the backdrop of its individual needs.[384] The question of how a company should go about creating its security plan has only one clear answer: it depends.[385] As the FTC Consent Orders and the GLB Security Rule indicate, factors such as the company's size and complexity, the nature of the company's activities, and the sensitivity of the personal information collected from consumers all must be considered.[386]

In general, the ability to design a plan to meet a company's specific needs is beneficial because a strategy that works well for one business may not work as well, or may be cost prohibitive, for another.[387] Specific legislation, however, defines the minimum standards that companies in particular industries must meet.[388] Therefore, before developing an appropriate information security policy, a company needs

---

management needs to be approached from a top-down perspective in the same way that accounting practices, compensation decisions, and corporate governance are. Mellon Financial, Novell, Home Depot, Procter & Gamble, Wal-Mart, and FedEx have all created IT governance committees similar to their audit, compensation and governance committees. *Id.*

383. *See* WESTBY, SECURITY, *supra* note 67, at 154 (suggesting business may not be able to occur if information systems cannot be trusted).

384. WESTBY, *supra* note 23, at 2.

385. Nolan & McFarlan, *supra* note 379, at 98.

386. *See, e.g., In re* BJ's Wholesale Club, Inc., No. C-4148, 2005 FTC LEXIS 134, at *6 (Sept. 20, 2005), *available at* http://www.ftc.gov/os/caselist/0423160/092305do0423160.pdf; 16 C.F.R. § 314.3(a).

387. Nolan & McFarlan, *supra* note 379, at 98.

388. In addition to the legislation discussed in Part III, other legislation might also dictate, at least in part, the security and privacy standards a company needs to meet. The Children's Online Privacy Protection Act protects personal information belonging to children under the age of thirteen. 15 U.S.C. §§ 6501-6506 (2006). The Electronic Communications Privacy Act might apply to Internet Service Providers and telephone companies. 18 U.S.C. §§ 2701-2712 (2006). The Economic Espionage Act of 1996 protects the privacy of trade secrets. 18 U.S.C. §§ 1831-1839 (2006). The Sarbanes-Oxley Act applies to corporations and contains provisions regarding data retention and destruction, as well as internal controls pertaining to financial information. Pub. Law 107-204, 116 Stat. 745 (codified at 15 U.S.C. §§ 7201-7266).

to identify applicable legislation[389] and determine what that legislation requires. After legal requirements are identified, a company should evaluate its own business needs.[390] Two business needs common to most companies dealing with personal information are making sure that customers feel confident that their personal information will be protected, and protecting data valuable to the business's operations.

In developing a strategy for handling private consumer information, the GLB Privacy Rule and the HIPAA Privacy Rule both present valuable ideas. While the GLB Privacy Rule applies only to financial institutions,[391] other companies might inspire trust in their consumers by offering similar privacy notifications voluntarily. Cost must also be considered in the development of a company's security plan.[392] Additionally, a company should not make any promises regarding consumer privacy that it cannot keep.[393] While the HIPAA Privacy Rule as a whole may not be part of a company's security plan if it is not required, some of its principles are likely applicable. One of the most effective methods of preventing identity theft is to avoid collecting information that is not needed.[394] The HIPAA Privacy Rule's "minimum necessary" policies limit disclosure of personal information to only the amount necessary to fulfill a given task.[395] In particular a company should avoid collecting and storing social security numbers, drivers license numbers, and other identifiers.[396] Finally, as suggested by the GLB Privacy Rule, a company should be aware of its promises to consumers when negotiating contracts with third parties.[397]

Additionally, a company should conduct a risk management assessment to determine existing risks, the likelihood of attacks, and

389. In addition to the federal legislation discussed here, a company must be conscious of applicable state laws and international laws that might affect it based on its industry. *See* Prepared Remarks of Brad Smith, Senior Vice President, General Counsel and Corporate Secretary, Microsoft, to Congressional Internet Caucus (Nov. 3, 2005) [hereinafter Smith Remarks] (on file with author), *available at* http://www.microsoft.com/presspass/press/2005/nov05/11-03DataPrivacyPR.mspx (follow "Brad Smith Address to Congressional Internet Caucus" hyperlink under "Executive Speeches") (over 20 states have passed financial privacy laws since 2004).

390. *See* Nolan & McFarlan, *supra* note 379, at 96.

391. 15 U.S.C. § 6809 (2006).

392. *E.g., id.* § 3544(a)(2)(C) (stating FISMA requires the implementation of "cost-effective methods").

393. *See, e.g., In re* Guess?, Inc., No. C-4091, 2003 FTC LEXIS 123 (July 30, 2003), *available at* http://www.ftc.gov/os/2003/08/guessdo.pdf. (prohibiting misrepresentation of privacy protection).

394. *See* Shostack Letter, *supra* note 345.

395. 45. C.F.R. § 164.514(d)(2) (2006).

396. *See* Shostack Letter, *supra* note 345.

397. 15 U.S.C. § 6802(b)(2) (2006).

proper recovery methods.[398] While the GLB Safeguards Rule only applies to financial institutions, the FTC has recommended that Congress consider extending it to all companies, regardless of whether or not they are financial institutions.[399] As suggested by the GLB Security Rule and the FTC Consent Orders, an effective risk assessment should result in the creation of administrative, technical, and physical safeguards aimed at protecting the security, confidentiality, and integrity of data.[400] Specific safeguards are dependent upon the business needs of an individual organization and the best practices of its industry.[401] Regardless of the specific safeguards that are implemented, employee training, network and software design, data storage, data transmission, attack response and prevention, hardware security, and employee access should all be addressed.[402]

Even though compliance with FISMA by covered government agencies is not as good as the federal government would like,[403] its accountability requirements should be considered by a company developing a security plan. FISMA places ownership of an agency's information security program with one person.[404] Likewise, a company should assign ownership and responsibility for the implementation of its security plan, although developed from an organizational standpoint, to one person or office. In addition to executing the security plan, this person, with proper input from management, should be charged with the continual development and refinement of the organization's risk management plan.[405] The security plan should be audited by both internal and external sources. An effective security plan should provide for outside audits by a qualified individual or organization on a regular basis.[406] The organization's security plan must grow with the organization and respond to changes in technology.

---

398. WESTBY, *supra* note 23, at 22.

399. Press Release, U.S. Fed. Trade Comm'n, FTC Testifies on Data Security and Identity Theft (June 16, 2005) *available at* http://www.ftc.gov/opa/2005/06/datasectest.htm.

400. 16 C.F.R. § 314.3(a) (2006). *See also In re* BJ's Wholesale Club, Inc., No. C-4148, 2005 FTC LEXIS 134, at *4 (Sept. 20, 2005), *available at* http://www.ftc.gov/os/caselist/0423160/092305do0423160.pdf.

401. *See* Nolan & McFarlan, *supra* note 379, at 96 (describing four strategies an organization might employ based on the strategic impact of IT on the organization).

402. *See In re* BJ's Wholesale Club, Inc., 2005 FTC LEXIS 134, at *5. *See also* 45 C.F.R. §§ 164.310 and 164.312.

403. *Cybersecurity Report*, *supra* note 248.

404. 44 U.S.C. § 3544(a)(3) (2006).

405. *See* Tower, *supra* note 341 (describing charges filed against a company that failed to appropriately adjust its security measures to reflect changes in its technology).

406. The FTC Consent Orders require independent audits at least every other year. *See, e.g., In re* BJ's Wholesale Club, Inc., 2005 FTC LEXIS 134, at *5-6.

Even the best security plan and most effective implementation and management do not guarantee that a corporation will avoid a data security breach.[407] A cyber-insurance policy helps a company protect itself from risks that could not be determined from the risk management assessment and risks that the security plan was designed to stop, but did not.[408] Cyber-insurance is relatively new and risk can be difficult to determine because the interconnected nature of information systems presents risks beyond the individual company.[409] As a result, underwriters are hesitant to write large policies.[410] However, as underwriters gain more experience in the area of cyber-insurance, larger policies will become available to supplement a company's security policy.[411]

Finally, if a security breach does occur, a company should contact the customers who are affected or potentially affected.[412] Since consumers might not discover identity theft until months or years after the theft occurs, failure to disclose potential data breaches hinders the fight against cybercrime.[413] Although a company might be reluctant to disclose information that might harm its public image, disclosure would not only make recovering from identity theft easier for affected customers, it would also minimize the company's exposure. Disclosure is already required by law in California[414] and federal bills requiring disclosure are being considered by Congress.[415]

B. Uniform Legislation: The Need For Minimal Requirements

> [P]ersonal information collected at a bank is covered by one privacy standard, but that same information collected by a hospital is covered by a different standard. If that information is from a child under the age of 13, it's protected by yet another standard if it's collected online, but it may not be protected at all if it's collected offline. . . .

---

407. Lawrence A. Gordon, Martin P. Loeb, & Tashfeen Sohail, *A Framework for Using Insurance for Cyber-Risk Management*, 46 COMM. ACM 81, 84 (2003).

408. *Id.*

409. *Id.* at 82-84.

410. *Id.* at 84.

411. *Id.* at 83.

412. *When ID Theft Hits: What to do*, MSNBC ONLINE, Feb. 28, 2003, http://www.acm.org/usacm/Issues/WhenIDthefthits.htm (last visited Jan. 28, 2006) (delays in closing accounts can be costly for victims of identity theft).

413. WESTBY, SECURITY, *supra* note 67, at 150 (information sharing is an important component of cyber security).

414. CAL. CIV. CODE § 1798.29 (West 2006) (requiring notification of a data breach that puts personal information at risk to any citizen of California).

415. *See, e.g.*, Notification of Risk to Personal Data Act of 2005, S. 751, 109th Cong. (2005) (requiring all persons engaged in interstate commerce to disclose data breaches containing personal information).

> Yet, despite all of these legal distinctions, the consequences of misuse [of personal information] . . . could be exactly the same in each scenario.[416]

Although some common standards emerge from existing legislation, there is still much confusion in the area of data security.[417] In some industries, such as health care, the law requires strict compliance with very specific standards.[418] Yet in other instances, there is little or no applicable legislation. Data security standards also can be different within an industry.[419] Regardless of how a company collects private information or the nature of the company's relationship with the owner of the information, once a company collets data it is often all stored in the same databases and transported over the same networks.[420] Federal legislation establishing minimal data security standards for personal information would force all companies to take data security seriously.

On the other hand, legislation that is too inclusive could be cost prohibitive and ineffective.[421] Some suggest the HIPAA Safeguards Rule created confusion in the health care industry.[422] Although the goal of HIPAA is to make electronic transfers more prevalent and reduce costs,[423] implementation of new security policies is costly in itself. Further, companies cannot yet look to standards boards for data security rules in the same way they can look to accounting standards boards for accounting rules.[424] While these standards boards are beginning to develop,[425] some argue that standards boards need to be allowed to set ground rules before Congress intervenes with uniform data security requirements.[426]

Any forthcoming legislation must walk the line between providing effective data security and crippling the advantages created by the Internet and e-business. If legislation is too specific, businesses may not be able to effectively interact with legitimate customers. Without a uniform baseline for data security standards, however, the confusion that

---

416. *See* Smith Remarks, *supra* note 389.

417. *Id.* (discussing inconsistency between different federal and state laws).

418. *See* 45 C.F.R. §§ 160, 162, 164 (2006).

419. *See* 15 U.S.C. § 6809 (2006) (requiring different levels of protection for "consumers" and "customers").

420. *See, e.g.,* Complaint at *2, *In re* Guess?, Inc., No. C-4091, 2003 FTC LEXIS 123, (July 30, 2003), *available* at http://www.ftc.gov/os/2003/08/guesscomp.pdf.

421. *See* WESTBY, PRIVACY, *supra* note 67, at 44.

422. *Id.* (arguing that government needs to better understand cyber security before passing legislation).

423. WESTBY, SECURITY, *supra* note 67, at 38.

424. Kevin Novack, *Reconsider Cybersecurity Regulation,* NETWORK COMPUTING, Oct. 30, 2003, at S12.

425. *See supra* note 382 and accompanying text.

426. Novack, *supra* note 424, at S12.

currently exists will continue, and businesses not currently covered by legislation will have little incentive to spend time and money developing data security systems. While a uniform minimum level of data security is needed, some information is more sensitive and requires additional considerations. Legislation such as HIPAA and the GLB Act could still provide greater protection for specific industries than a uniform standard would require.

Uniform legislation should revolve around four considerations. First, data is data, regardless of how it is collected or the nature of its owner's relationship to the collecting entity.[427] Uniform legislation should apply consistent standards to personal information, based on the sensitivity of the information. Second, a one-size-fits-all approach to data security will not work. Therefore, uniform legislation should require management to create data security policies, but not dictate what technology must be used or specify methods by which policies must be implemented.[428] While the legislation should be flexible, it also must have strong enforcement policies.[429] Third, if data is never in harm's way, it cannot be stolen. Uniform legislation, like HIPAA's "minimum necessary" standard, should limit the type of personal information collected to that which is necessary. If a company does not have a legitimate business need for specific information, it should not collect it. Fourth, uniform data security legislation should require a company to notify consumers if it suffers a data breach and consumers' personal data is exposed or potentially exposed.[430] No data security program can provide total protection against a data breach.[431] However, the quicker a potential identity theft victim learns he or she has been victimized, the sooner he or she can fight back. Uniform legislation that addresses these concerns, while at the same time gives businesses flexibility in developing an appropriate data security plan, will provide clarity in the area of data security without frustrating the benefits technology brings to today's business environment.

427. *See* Smith Remarks, *supra* note 389 (suggesting the potential risks to consumers are the same regardless of how data is collected).

428. *See* 16 C.F.R. § 314.3(a) (2006) (suggesting that an information security program should be appropriate for a company's size, complexity, industry, and activities).

429. *See* WESTBY, PRIVACY, *supra* note 67, at 45 (suggesting compliance with HIPAA is taken seriously because criminal and civil penalties exist).

430. *See* CAL. CIV. CODE § 1798.29 (West 2006).

431. *See* Gordon, Loeb & Tashfeen, *supra* note 407, at 84.

VI. Conclusion

Technology has changed the way business is done. With these changes come new challenges. It is undeniable that information drives business today, even in spite of existing challenges.[432] When a bank robber named Willie Sutton was asked why he robbed banks, he replied, "[b]ecause that's where the money is."[433] Today, information has replaced money and databases have replaced banks. Safes and locks have been replaced by encryption and firewalls, but the need for effective security and the potential for harm is just as great, if not greater. While identity theft existed and was a problem even before the birth of the Internet, recent data breaches have called attention to the fact that technology allows thieves to exploit more victims in less time than ever before.[434]

Even if we ignore the fact that technology changes at a rapid pace, effective data security is very dependent upon each individual company's business, making a one-size-fits-all approach to information security unworkable. Legal standards must be flexible enough to apply to different businesses, yet strict enough to effect compliance. The Internet has destroyed barriers to entry and opened the marketplace, allowing companies of all sizes to compete in the virtual business world. The challenge for future legal standards is to strike a balance that allows the advantages currently provided by e-business, while encouraging all companies to effectively protect consumer information.

The fight to control identity theft requires corporations to take data security and customer privacy seriously.[435] Effective laws can encourage corporate participation. However, corporate responsibly is only half of the battle. Consumers need to take proactive measures to protect themselves from identity theft.[436] Users transmitting data online need to educate themselves about Internet security.[437] Consumers should look for privacy policies on websites, read them, and do business only with reputable companies.[438] Internet users should install firewalls and virus protection programs on their computers and update these regularly.[439] Consumers should opt out of third party information sharing and be selective about distributing personal information.[440]

---

432. WESTBY, *supra* note 23, at 12.
433. Levy & Stone, *supra* note 1.
434. *See id.*
435. *See* WESTBY, *supra* note 23.
436. Reducing the Risk, *supra* note 35.
437. *Id.*
438. *Id.*
439. *Id.*
440. *Id.*

It is clear that any business collecting or storing its consumers' personal data has to take steps to adequately protect that data. However, the legal duty that currently exists varies drastically by industry.[441] Further, the applicable legal duty is often unclear as new technology creates new legal questions.[442] The enactment of uniform legal standards can provide a starting point in the battle to secure personal data and force businesses to develop security plans. However, the problems associated with securing personal information will not be remedied without an active commitment by the business community and the consuming public to attack the problem from a practical standpoint as well as a legal standpoint.

441. *See generally supra* Part III.

442. *See, e.g.*, Sovereign Bank v. BJ's Wholesale Club, Inc., 395 F. Supp. 2d 183, 187 (M.D. Pa, 2005).